Relatively Concise Notes on Securing Exchange 2000 Servers and Active Directory Domain Controllers using Templates

These notes refer to the situation of installing a new Windows 2000 Active Directory (AD) domain controller (DC2) and Exchange 2000 server (EX4) into an existing AD/Exchange environment. The environment includes a strong commercial departmental firewall. Firewall rulesets will not be addressed. The primary methodology is culled from the NSA's "Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set" and the NSA's "Guide to the Secure Configuration and Administration of Microsoft Exchange 2000", used in combination with Microsoft's "Security Operations Guide for Windows 2000 Server" and "Security Operations for Microsoft Exchange 2000 Server". Also used and blended were portions from the following Group Policy templates:

- Microsoft BaselineDC.inf (downloaded with the Security Operations Guides referenced above).
- Microsoft Exchange BackEnd Incremental.inf (also from the Operations Guides)
- NSA: w2k_server.inf along with NSA supplied instructions for Exchange 2000 (see instructions)

The results of this effort are these (slightly) customized templates:

- **For Exchange:** SEWP_NSA_w2k_server_conf_for_exchange.inf
- **For DCs**: SEWP_BaselineDC.inf

The templates are applied via Group Policy at the OU level.

Further Background:

(1) The Outlook Web Access (OWA) architecture is two tier, front-end/back-end. The front-end server had previously been configured and is not in the scope of this document. Briefly though, the "Security Operations for Microsoft Exchange 2000 Server" guide was followed. The baseline.inf and OWA FrontEnd Incremental.inf templates were applied. IIS Lockdown was run using the OWA template with URLScan also being applied. An IPSEC policy was configured to allow only local domain activity (for NT Logons), 443 (SSL only), and a required ESP connection to each of the Exchange servers for port 80—providing full transport mode protection of the connection between the front-end and back-end servers.

(2) There are no "downlevel" clients in the environment (no 98 or NT). All clients are XP or 2000. Office software is predominately at XP level.

Exchange Server

Disk/Partition Security ACLs:

- Exchange was installed in its own Program Files directory on its own disk partition (E:).

- Exchange Log Files were place on their own partition (F:, which is RAID 1).
- The Exchange DB files were places on their partition (G:, which is RAID 5).

The following partition ACLs were set for E:, F:, and G:

- System (Full Control)
- LOCAL_EXCHANGE_MACHINE_NAME (Full Control)
- Domain Admins (Full Control)
- Authenticated Users (Read & Execute).

IPSEC Policy:

- Created initial IPSEC ruleset via export, importing, and modifying previously configured exchange server IPSEC ruleset.
- Allows all local net connection for users, other exchange servers, and domain controllers
- Only accepts port 80 connection from OWA servers and requires this connection to be protected via ESP.
- Also updated a local Blackberry Enterprise server to have connectivity to this exchange machine.
- Blocked all other access.

Exchange Configuration:

- Exchange installed on own partition (E:)
- Installed SP3.
- Moved Logs to their own partition (F:)
- Private and Public message stores to separate partition (G:).
- SMTP server, renamed our sending domain to –EX4.sewp.nasa.gov, defined a SMARTHOST to internet-facing-server.sewp.nasa.gov, checked "Attempt direct delivery…" so that mail to other local sewp_domain servers is direct.
- OWA: setup sewpmail virtual directory, enabled "Exchange Path, Mailboxes for" sewp_domain.sewp.nasa.gov (access the whole domain, not just one server, required for OWA).
- Deletion Setting (Mailbox store property). Set/confirmed: Keep deleted items/15 days, Keep deleted mailboxes/30 days, checked "Do not permanently delete items/mailboxes until the store has been backed up"
- Messages tracking enabled via server properties. Checked "Enable subject logging and display" and "Enable message tracking"
- Enabled SMTP extended logging: Date, Time, Client IP, User Name, Method, URI Query.
- Enabled Full Text indexing…configured index to be at G:\ExchangeServer_EX4\Projects. Enabled to run updates at 20:00 daily. Used information on pp. 268-269 of the "Exchange 2000 Server 24seven" book.

Security Other:

- Virus Scanning: Version 6.2 of TrendMicro ScanMail for Exchange 2000. Configured for real time scan, and full stores scan nightly at 0400. Configured for virus definition update hourly.

Backups:

- Until a 3rd party backup client is installed NTBACKUP will be used.
- Scheduler service was enabled to support backups. Note: since the "Removable Storage" service is disabled, NTBACKUP will generate a warning at startup. Make sure to check "Do not display message again" at least once to allow the scheduled backups to run.
- The initial target of system backups is a share in <otherserver>. There is a 100GB partition available (RAID 5) for backups.
- System backups will write to share Sysbackups$
- Exchange backups will write to share Exbackups$
- Only administrators have any access to these shares
- Whenever there is a significant system configuration change a full system backup, titled "fullsystemmmddyy.bkf" will be written to the Sysbackups$ share. Also, an Emergency Repair Disk (floppy) will be created.
- Daily exchange backups will be done Monday through Saturday. They are titled Ex4Storesxxx.bkf where xxx is Mon…Sat.
- Daily System State backups are done Monday through Saturday. They are titled Ex4SSxxx.bkf where xxx is Mon…Sat.

Domain Controller

DC Configuration Steps:

- DCPromo
- Configured as a Global Catalog
- Configured time services (in anticipation of being FSMO PDC Emulator master). Used the net time /setsntp: command. Also followed Q articles 216734 and 307937 to enable additional time logging (the default is minimal time logging of failures, these articles provide for extended logging including successful attempts).
- An internal DNS was configured with forwarding set up to external DNS.

IPSEC Policy:

- Created initial IPSEC ruleset via export, importing, and modifying previously configured domain contoller IPSEC ruleset.
- Allows all local net connection for users, other exchange servers, and domain controllers
- Blocked all other access.

Templates

Changes to supplied templates are documented but are not guaranteed to be complete
.

For Exchange: SEWP_nsa_w2k_server_conf_for_exchange.inf—SEWP modifications:

User Rights Assignment	
Access this computer from the network	Add: Authenticated Users, Backup Operators, ENTERPRISE DOMAIN CONTOLLERS
Manage auditing and security log	Add: <local domain>\Exchange Domain Servers
Local Policies/Security Options	
Number of previous logons to cache (in case domain controllers is not avaiable)	3
Shut down system immediately if unable to log security audits	Disabled
System Services	
Iisadmin	Automatic
Imap4svc	Disabled
IPSEC Policy Agent	Automatic
msexchangees	Disabled
msexchangeIS	Automatic
msexchangemgmt	Automatic
msexchangemta	Automatic
msexchangesa	Automatic
msexchangesrs	Disabled
mssearch	Automatic
NT LM Security Support Provider	Automatic
Pop3svc	Disabled
Remote Procedure Call (RPC) Locator	Automatic
Resvc	Automatic
SMTPSVC	Automatic
Task Scheduler	Automatic
TermService	Automatic
W3SVC	Automatic
Windows Management Instrumentation	Automatic

For DCs: SEWP_BaselineDC.inf—SEWP modifications:

Local Policies/Security Options	
Digitally sign client communication (always)	Disabled
Digitally sign server communication (always)	Disabled
LAN Manager Authentication Level	Send LM & NTLM –use NTLMv2

	session security if negotiated
System Services	
IPSEC Policy Agent	Automatic
Print Spooler	Automatic
Task Scheduler	Automatic
TermService	Automatic
Windows Management Instrumentation	Automatic